International Journal of Mathematics and
Computer Applications Research (IJMCAR)
ISSN (P): 2249-6955; ISSN (E): 2249-8060
Vol. 9, Issue 1, Jun 2019, 11-16
© TJPRC Pvt. Ltd.

TRANS STELLAR
•Journal Publications •Research Consultancy

ENHANCED IDENTITY-BASED CERTIFICATELESS SIGNCRYPTION SCHEME

V. ISAKKIRAJAN[1] & M. RAMAKRISHNAN[2]

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India*

[2]*Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India*

ABSTRACT

Secure Internet communication can be made more efficient using a Crypto System called identity-based certificateless signcryption scheme and constructing a secure one is a challenge, which is achieved using a standard model. The primary aim of this paper is to securely generate keys and for encryption and decryption functions. Strong security, better performance efficiency and reduced cost expanses are all made possible by the enhanced new system.

KEYWORDS: Identity-Based Encryption, Certificateless, Signcryption, Cryptography, Encryption & Decryption

Received: Dec 19, 2018; **Accepted:** Jan 09, 2019; **Published:** Jan 22, 2019; **Paper Id.:** IJMCARJUN20193

Original Article

INTRODUCTION

A new method was developed in the year 1977 by Cryptographers Ron Rivest, Adi Shami and Leonard Adleman, which comprised the use of two keys, private key and public key. According to the new method, the private key as the name says will be known only to the owner and public key can be shared with everyone. This method involves a complex mathematical formula involving huge number of prime numbers and exponentiations[I]. The challenge in the field of cryptology is that cryptographers always endeavor to find new ciphers that are increasingly tough to break, and cryptanalysts work to break the ciphers. Initially there used to be only a single key used by both the sender and the receiver to encrypt a message, thereby making it tough to break the ciphers. In instances when there is a doubt among the receiver and sender with regard to the security of their connection, they avoid/stop using cryptography to encrypt their messages. Apart from this issue, since both sender and receiver have only one key, they first need to meet and exchange a common key so that each other's messages are decrypted. This becomes a major problem if the sender and receiver are unable to meet in person.

In the new method, the public and private keys are generated by the server followed by the Internet publishing the public key. However, using the public key if a hacker hacks the server and replaces the server's public key with the hacker's public key, then the hacker could intercept the incoming cipher text messages and decrypt them. This can be proactively avoided by a new mechanism called, certificates.[II] Using the public and private key pair, an individual can encrypt a message with his or her private key and using the individual's public key the message can be decrypted. As the person's public key decrypts the message, the corresponding private key must have encrypted it, so anyone who decrypts the message knows that the person sent it. The new method is known as Signing and the Crypto and together it is called as Signcryption.[VII]

Certificates for a server are generally issued by a trusted party called a certificate authority or CA. The certificate consists of the public key of the server encrypted with the private key of the signer. At the time of browsing, the public key issued by the CA will be embedded in their code and these keys can be trusted at the root

level, assuring that system security has not been hacked.

To avoid site certificates, the server can be displaced with identity-based encryption. For example, to buy a production from online, the individual browser connects to the server and downloads the certificate, which in turn verifies whether it has been signed by a trusted party and extracts the public key of the server. The public key encrypts the data and sends it to the server, which decrypts the data and completes the transaction. The main disadvantage to this scheme is that certificates rely on the user to manage them, but most web users are ignorant of the technology and the certificate concept. These days due to Internet insecurity, it becomes a must to check the certificates and can cancel the certificate if required. This study demonstrates the use of signcryption authentication system [VIII] by avoiding certificates for encryption.

The paper consists of the following sections: implement server socket language for certificateless encryption, private key generation method using RSA, extended Euclidean method for signcryption authentication, sender and receiver method.

FRAMEWORK FOR IDENTITY-BASED ENCRYPTION SCHEME

In the identity-based encryption system, there would be only one certificate for the server, that is, the master certificate embedded in web browsers for the PKG.[IV] The server need not have its own certificate but requires the private key from the PKG to decrypt any message sent to it. Figure is the graphic representation of the process involved.

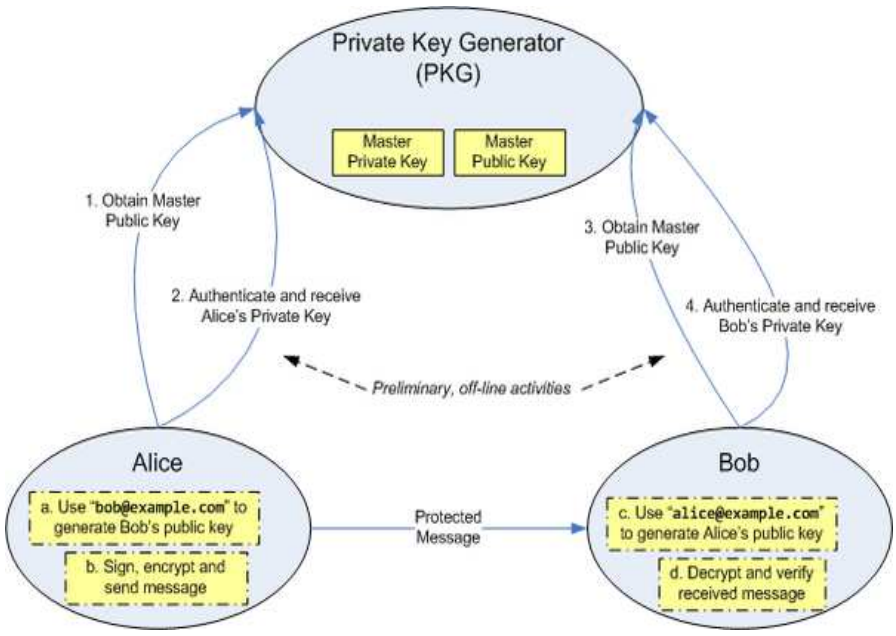

Figure 1: ID-Based Encryption: Off-line and Online Steps

To eliminate the need for certificates, a method of using identity-based encryption in SSL was adopted. For the server to be connected to PKG, to obtain its private key, and to encrypt the public key, a proof-of-concept code needs to be set up.

Identity-Based Encryption Using SSL Implementation

This section is about applying the identity-based encryption system to a traditional SSL implementation by showing a proof of concept.[IX]Main functions of the implementation are described below.

Private Key Generator Methods

Using RSA, PKG generates the public and private keysthat correspond to an ID which could be a "Domain Name". The following section shows as to how RSA generates public key and private key.[IX]

The RSA Algorithm Keys are Generated in the Following Manner

- p and q are selected using a primality test as the two distinct prime numbers.
    - For security purposes, the integers p and q should be chosen at random, with similar magnitude but different length, that is, by a few digits to make factoring harder.[2]
- Compute n = pq.
    - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute $\lambda(n) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p - 1, q - 1)$, where λ is Carmichael's totient function. This value is kept private.
- Choose an integer e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; i.e., e and $\lambda(n)$ are coprime.
- Determine d as $d \equiv e^{-1} \pmod{\lambda(n)}$; i.e., d is the modular multiplicative inverse of e modulo $\lambda(n)$.
    - This means: solve for d the equation $d \cdot e \equiv 1 \pmod{\lambda(n)}$.
    - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $e = 216 + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[14]
    - e is released as the public key exponent.
    - d is kept as the private key exponent.

The *public key* consists of the modulus *n* and the public (or encryption) exponent *e*.

The *private key* consists of the private (or decryption) exponent *d*, which must be kept secret. *p*, *q*, and $\lambda(n)$ must also be kept secret because they can be used to calculate *d*.

EXTENDED EUCLIDIAN METHOD

```
public BigInteger extendedEuclid(BigInteger a, BigInteger b) {
        BigInteger x = BigInteger.valueOf(1);
        y = BigInteger.valueOf(0);

        BigInteger xLast = BigInteger.valueOf(0);
        yLast = BigInteger.valueOf(0);

        BigInteger q, r, m, n;

        while(a.compareTo(BigInteger.valueOf(0)) != 0) {

        q = b.divide(a);
```

```
r = b.remainder(a);
m = xLast.subtract(q.multiply(x));
n = yLast.subtract(q.multiply(y));

xLast = x;
yLast = y;

x = m;
y = n;
b = a;
a = r;

}

if(xLast.compareTo(BigInteger.valueOf(0))<0)
xLast= Last.add((this.p.subtract(BigInteger.ONE)).multiply(this.q.subtract(BigInteger.ONE)));

returnxLast;

}
```

Using this method, the modular inverse of a number with respect to a number that is relative prime to it was found. [X]

Sender Methods

The Private Key Generator provides the ID of the receive and MESSAGE which is to send by Sender, then receiver receive the public key corresponding to the ID of receiver in which p*q. The MESSAGE can be encrypted by public key with RSA algorithm and the encrypted message is stored with Sender ID in a file, "encryptedmessage.txt".[V]

Encrpyt message using $C = M^e \bmod n$ where $0 \leq M < n$.

```
privatebyte [] messageEncrypt(byte [] message){
    byte [] EncryptMessage = (new BigInteger(message)).modPow(Public_key,
    n).toByteArray();
    return EncryptMessage;
    }
```

Receiver Methods

It is believed that PKG provides the ID and the respective private key of the receiver. Encrypted messages along with sender ID form the file "EncryptedMessage.txt".[VI]

Decrpyt message using $M = C^d \bmod n$.

```
publicbyte[] decryptMessage(byte[] encrptedmessage) {
        byte[] message = (new BigInteger(message)).modPow(private_key, n).toByteArray();
        return message;
 }
```

This function will return the message in byte form, which needs to be converted into a string form.

Identity-based encryption is more powerful than PKI because of the following:

Does not require any certificates and certificate management, hence

- no certificate server
- no certificate lookups for the client
- no certificate (or key) revocation, CRLs, OCSP etc.
- uses short-lived keys.

However, all the above mentioned cannot be avoided in case of PKIas this would compound lookup problem; PKI requires pre-enrollment

In PKI, for the sender to encrypt the message, the recipient must generate key pair

Using the identity-based encryption, which is ad hoc capable, a sender can send message at any time

- Identity-based encryption eliminates encryption key recovery/escrow server
    - Most PKI applications require access to private keys (e.g. Lost keys, Financial Audit, Virus Filtering etc.)
    - Key server can generate any key on the fly

CONCLUSIONS

Since it needs pre-enrollment, issuing certificates and also functions fine for authentication, and is powerful for encryption, identity-based encryption is considered the most expensive to be deployed and run. However, its security aspects can be made more efficient using smart cards. Identity-based encryption does not ask for pre-enrollment, is used only in software, and requires no key lookup, making revocation and content scanning easy.

REFERENCES

1. *Craig Gentry Certificate-Based Encryption and the Certificate Revocation Problem Advances in Cryptology - Proceedings of EUROCRYPT 2003 (2003)*
2. *Lee, Byoungcheon; Boyd, Colin; Dawson, Ed; Kim, Kwangjo; Yang, Jeongmo; Yoo, Seungjae (2004). Secure Key Issuing in ID-based Cryptography. ACS Conferences in Research and Practice in Information Technology - Proceedings of the Second Australian Information Security Workshop-AISW 2004. CiteSeerX 10.1.1.6.337.*
3. *SS Al-Riyami, KG Paterson Certificateless Public Key Cryptography Advances in Cryptology - Proceedings of ASIACRYPT*

2003 (2003)

4. *Adi Shamir, Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53, 1984*
5. *Sattam S. Al-Riyami and Kenneth G. Paterson, Certificateless Public Key Cryptography, Lecture Notes in Computer Science, pp. 452 – 473, 2003*
6. *D. Galindo. Boneh-Franklin Identity Based Encryption Revisited. In ICALP 05, LNCS 3580, pages 791–802.*
7. *Jianhong Zhang, Zhipeng Chen, Min Xu "On the Security of ID-based Multi-receiver Threshold Signcryption Scheme", In proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1944 – 1948, 2012.*
8. *Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption. Journal of Cryptology. 2007;20(2):203–235*
9. *Calderbank, Michael The RSA Cryptosystem: History, Algorithm, Primes 2007-08-20*
10. *Moon, T. K. (2005). Error Correction Coding: Mathematical Methods and Algorithms. John Wiley and Sons. p. 266*